

***AESDIRECT***  
**ACCOUNT ADMINISTRATION USER GUIDE**

Updated July 22, 2013

# TABLE OF CONTENTS

<b>Section</b>	<b>Page</b>
<b>OVERVIEW</b>	<b>3</b>
<b>AES<i>Direct</i> Roles Defined</b>	<b>3</b>
<b>AES<i>Direct</i> Rules</b>	<b>5</b>
<b>Username Rules</b>	<b>5</b>
<b>Password Rules</b>	<b>5</b>
<b>Session Rules</b>	<b>6</b>
<b>THE MANAGE USER FUNCTIONS</b>	<b>8</b>
<b>HOW TO</b>	<b>11</b>
<b>Create a New User</b>	<b>11</b>
<b>Create a User Manager</b>	<b>16</b>
<b>Reset Passwords</b>	<b>20</b>
<b>Disable a User</b>	<b>24</b>
<b>Reactivate a Disabled User</b>	<b>26</b>
<b>Reactivate a Locked Out User</b>	<b>31</b>
<b>Change an Account Administrator</b>	<b>37</b>
<b>WHAT HAPPENS IF THE ACCOUNT ADMINISTRATOR LEAVES?</b>	<b>41</b>

## OVERVIEW

### ***AESDirect* Roles Defined**

Each *AESDirect* Account includes three distinct types of Users, each with their own role to play in filing and their own set of responsibilities.

This Administrative Guide was created to help the Account Administrator and the User Manager understand fully their role in *AESDirect*. Users and those Account Administrators and User Managers who will file EEI should look to the ***AESDirect* User Guide** to understand that set of responsibilities.

#### ***Account Administrator***

The Account Administrator is responsible for the *AESDirect* account and should be a Customs Compliance specialists and a company officer.

An Account Administrator's responsibilities include:

Interacting with *AESDirect* - If there are changes to be made to your *AESDirect* Account which require interaction with *AESDirect* Technical Support, the Account Administrator must be the initiating party. The Account Administrator must be the signatory on all documents requesting any substantial change to an account.

Creating and Managing User Managers – The Account Administrator can create up to two User Managers to help in the day-to-day management of traditional *AESDirect* Users.

Creating and Managing Users - The Account Administrator, as the first User in *AESDirect*, is responsible for creating Users, providing those Users a Password and managing their access to your *AESDirect* Account, by manually resetting passwords or disabling accounts, when necessary. The Account Administrator may delegate this responsibility to a User Manager.

#### ***User Managers***

A User Manager is an *AESDirect* expert. A User Manager serves as a point of contact for those who wish to use a company's *AESDirect* account. A User Manager can do everything an Account Administrator can, such as create Users and manage their access. User Managers cannot act legally on behalf of the Account holder when contacting *AESDirect* or make any changes to the Account Profile.

Any new or existing User in your *AESDirect* Account can be a User Manager. Your Account is limited, however, to only two (2) User Managers.

## *Users*

Users hold the most fundamental role in *AESDirect*. They are responsible for the day-to-day filing of EEI. Users may also be limited to viewing historical filing data.

# AESDIRECT RULES

## Username Rules

Each User in *AESDirect* should have their own Username. To clearly identify each User and to provide equal access to all users, strict rules are in place for the creation of Usernames.

**Unique** - All *AESDirect* usernames must be unique across the *AESDirect* system, even between different companies. For example, Company ABC creates username 'JohnDoe.' Company XYZ cannot also create a 'JohnDoe.' They may, however, create a version of this username, such as 'JohnDoe123' if available.

**Complex** – Usernames must be alpha-numeric and between 3 and 25 characters long

**Usernames are Not Case Sensitive**

**One Life Only** – Once a username is created, it is permanently assigned to the company that created it, even if the user moves to a new company.

## Password Rules

*AESDirect* Password Rules are strictly enforced, in this case, to maximize security. Common words and phrases are not acceptable.

**Complex** – All passwords must be at least 12 characters long and contain characters from 3 of the following 4 groups:

- Lowercase letters
- Uppercase letters
- Numbers
- Non-alphanumeric characters (!, \$, #, % );

At least 6 of those characters may occur only once in the password

**Unique** – Passwords cannot contain any familiar words or sequential character strings. They must also vary significantly each time they are reset.

- Passwords cannot contain any string that is also contained in the username
- Passwords cannot contain any dictionary words
- Passwords cannot contain any common strings such as
  - A sequential series of letters (e.g. abcd)
  - A sequential series of numbers (e.g. 1234) or pattern of numbers (e.g. 2468)
- Password must be unique for 4 years

- Passwords must be unique within the last 24 passwords

**Temporal** - Passwords on standard User accounts will expire every 60 days. Each new Password must meet the above parameters. You will be notified each time you login of the number of days remaining until your password expires.

Passwords cannot be changed more than once per day.

## Session Rules

Every time you log in to *AESDirect*, a timer is activated. This timer serves both as a session regulator and an activity counter. To improve security, User Accounts may only be inactive for a finite amount of time, whether for an individual session, or the accounts lifespan.

### Account Inactivity

- Accounts will be deactivated if they have not been accessed by any Users in 30 days.
- Once deactivated, the Account Administrator will need to contact AESDirect Technical Support to have the Account reactivated.

### User Inactivity

- Users will be deactivated if they have not logged in for more than 30 days.
- E-mail warnings will be delivered to the User once a day after 25 days of inactivity. The E-Mail will remind of the need to change their password and direct them to the appropriate resources.
- Once deactivated, the Account Administrator or User Manager will need to reactivate the User

### Session Timeout



- All *AESDirect* User sessions will time-out after 15 minutes of inactivity. A pop-up will notify a User 5 minutes before time-out.
- Actions, such as opening a window or moving from one page to another, will reset the 30 minute timer

- Once inactive for more than 15 minutes, the User will be forced to log in again. All data that was not saved before the timeout will be lost

## Concurrent Sessions

- Each Username can be used for up to five simultaneous sessions. That is, a user can login to five different computers, or five different types of web browsers on one machine, at the same time.
- The sixth session attempt will fail. The attempt will be logged.

## Logout

[Need Help?](#)

Username:

Password:

**No user account found for the username and password entered**

You can try 3 more time(s) before your user account is locked out

Please check that you have entered the correct username and remember that passwords are case sensitive.

Contact your account administrator or a user manager if you need assistance.

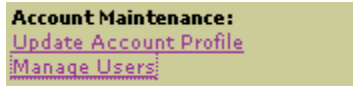
*Please remember that passwords are case sensitive. For users that have upgraded to the new account administration tools, 5 consecutive invalid login attempts will result in your username being locked out.*

- After 5 consecutive, invalid login attempts within 15 minutes the User will be locked out
- The locked out User can only be reactivated by the Account Administrator and only 15 minutes after the final failed login attempt

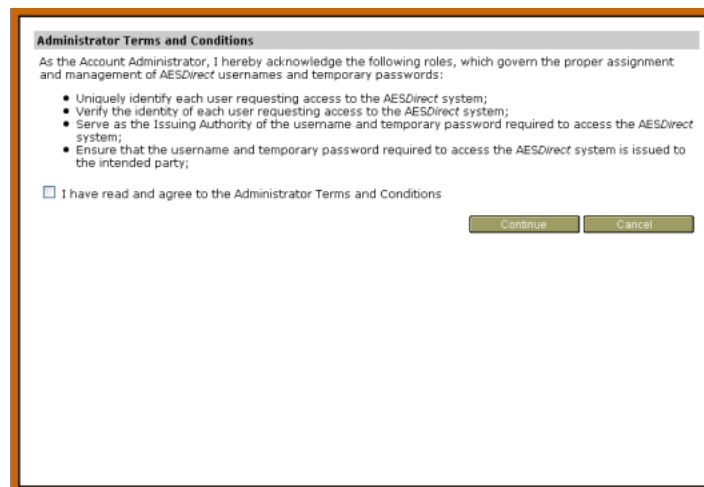
## THE MANAGE USERS FUNCTIONS

Account Administrators and Users Managers have access to the **Manage Users** screen and will see the link to those functions on the *AESDirect* interface.

To access the Manage User Functions...



Under **Account Maintenance**, click 'Manage Users'

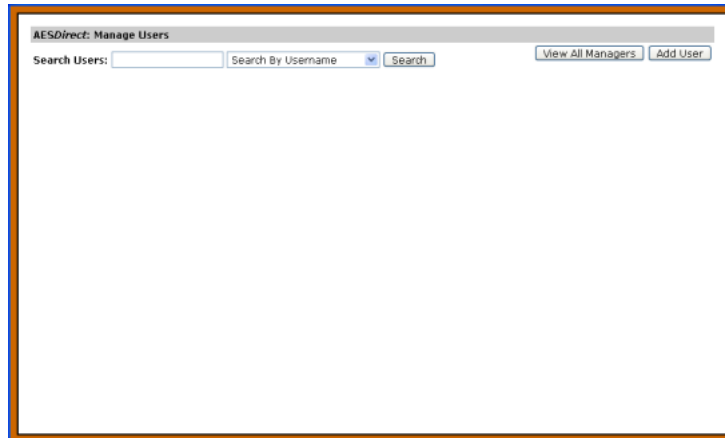
A screenshot of a dialog box titled 'Administrator Terms and Conditions'. The text inside reads: 'As the Account Administrator, I hereby acknowledge the following roles, which govern the proper assignment and management of AESDirect usernames and temporary passwords:'. Below this is a bulleted list of four roles: 'Uniquely identify each user requesting access to the AESDirect system;', 'Verify the identity of each user requesting access to the AESDirect system;', 'Serve as the Issuing Authority of the username and temporary password required to access the AESDirect system;', and 'Ensure that the username and temporary password required to access the AESDirect system is issued to the intended party;'. At the bottom left, there is a checkbox labeled 'I have read and agree to the Administrator Terms and Conditions'. At the bottom right, there are two buttons: 'Continue' and 'Cancel'.

If this is the first time you are accessing these functions, you will be asked to confirm the **Administrator Terms and Conditions**.

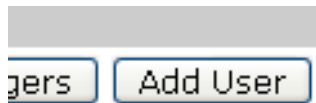
Check the box to acknowledge you have read and understood the Administrator Terms and Conditions.

Click 'Continue.'

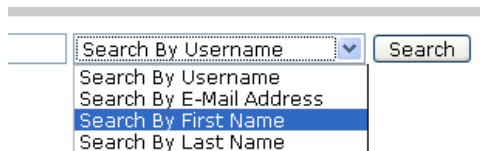




You will be brought to the **AESDirect: Manage Users** screen. From the **AESDirect: Manage Users** screen, you may add new Users as well as search for and modify existing Users.



Click ‘Add User’ to create a new User. Creating a User is as straight forward as filling in their information, choosing their permissions and then delivering their Username and Password.



Account Administrators can search for existing Users by one of these criteria:

- Username
- E-Mail Address
- First Name
- Last Name

Enter at least the first character of the search term and click ‘Search’ to return a list of matches.

Username	Quiz App Mgr Admin	First Name	Last Name	E-Mail Address	Expiration
test005	Y	Y	luba	l@l.com	12/14/2008
test006	DISABLED			l@l.com	-
test007	DISABLED	test		l@l.com	-
test100	DISABLED	gh		l@l.com	-
test1001	DISABLED	LUBA		l@l.com	-
test1002	DISABLED	luba		l@l.com	-
test1003	DISABLED	luba		l@l.com	-
test1004	DISABLED	lu		l@l.com	-
test1005	DISABLED	luba		l@l.com	-
test1006	DISABLED	luba		l@l.com	-
test1007	DISABLED	ll		l@l.com	-
test101	DISABLED	test		l@l.com	-
test1010	DISABLED	luba		l@l.com	-
test1011	DISABLED	luu		l@l.com	-
test1012	DISABLED	l		l@l.com	-
test1013	DISABLED	luba		l@l.com	-
test102	DISABLED			l@l.com	-
test103	DISABLED			l@l.com	-
test104	DISABLED			l@l.com	-
test201	DISABLED	luba		l@l.com	-

Easily identify the current status of a User, including their permissions or if they have been Disabled or Locked Out.

Sort the list of Users by clicking a highlighted column name, such as Username, First Name, Last Name and E-Mail Address.

## HOW TO...

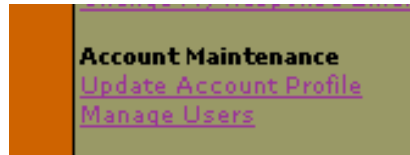
This section will help guide you through the step-by-step process of completing each administrative task in *AESDirect*.

### Create a New User

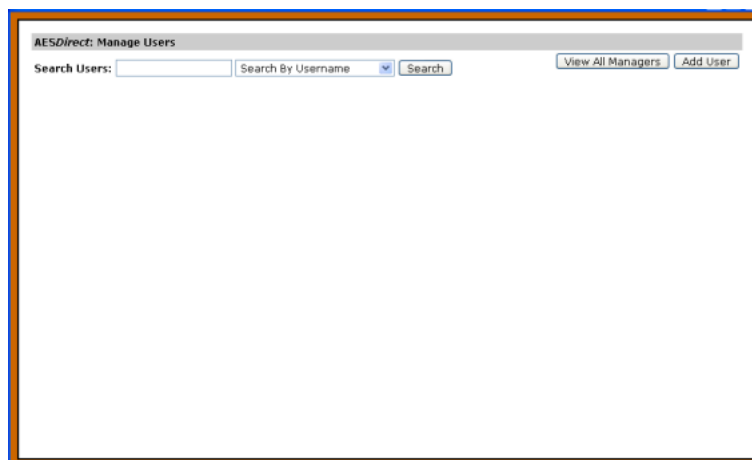
Users are the backbone of the *AESDirect* filing experience. Anyone who accesses *AESDirect* is a User. Users access the system with a Username and a Password to perform the tasks to which they are assigned. Usernames must be 3-25 characters in length. Passwords for Users expire every 60 days.

To create a New User...


- 1) Login to *AESDirect*



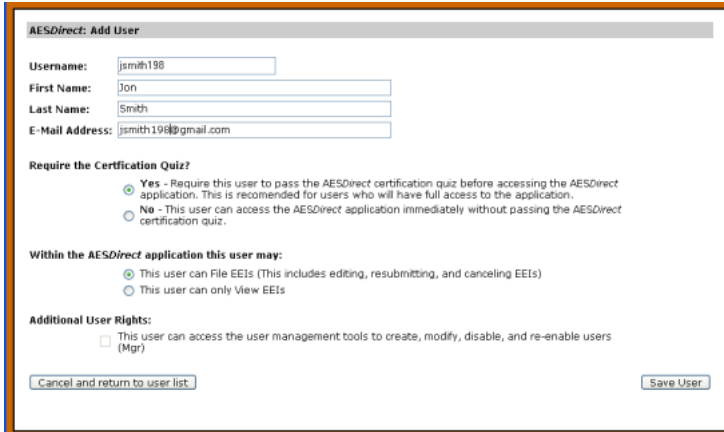
- 2) Under **Account Maintenance**, Click 'Manage Users'



- 3) The **AESDirect: Manage Users** screen will open

A rectangular button with a blue border and the text "Add User" in the center.

4) Click the 'Add User' button

A screenshot of the "AESDirect: Add User" web form. The form has a title bar "AESDirect: Add User". It contains several input fields: "Username:" with "jsmith198", "First Name:" with "Jon", "Last Name:" with "Smith", and "E-Mail Address:" with "jsmith198@gmail.com". Below these are three sections of radio button options. The first section is "Require the Certification Quiz?" with "Yes" selected. The second section is "Within the AESDirect application this user may:" with "This user can File EEIs" selected. The third section is "Additional User Rights:" with an unchecked checkbox for "This user can access the user management tools". At the bottom are two buttons: "Cancel and return to user list" and "Save User".

**AESDirect: Add User**

Username:

First Name:

Last Name:

E-Mail Address:

**Require the Certification Quiz?**

☒ Yes - Require this user to pass the AESDirect certification quiz before accessing the AESDirect application. This is recommended for users who will have full access to the application.

☐ No - This user can access the AESDirect application immediately without passing the AESDirect certification quiz.

**Within the AESDirect application this user may:**

☒ This user can File EEIs (This includes editing, resubmitting, and canceling EEIs)

☐ This user can only View EEIs

**Additional User Rights:**

☐ This user can access the user management tools to create, modify, disable, and re-enable users (Mgr)

The **AESDirect: Add User** screen will open

5) Enter a Username

The Username must be unique to *AESDirect*. If the Username already exists, you will be notified and given a chance to choose another Username.

6) Enter the User's First Name

7) Enter the User's Last Name

8) Enter the User's E-Mail Address

9) Under **Require the Certification Quiz?**

- a) Choose 'Yes' if you want to require the User to take and pass the *AESDirect* Certification Quiz before accessing the *AESDirect* application. This is highly recommended.
- b) Choose 'No' if you do NOT want to require the user to take and pass the *AESDirect* Certification Quiz before accessing the *AESDirect* application.

10) Under **Within the AESDirect application this user may:**

- a) Choose 'File EEI' which will give them permission to Create, File and Edit EEI
- b) 'Only View EEI' which will give the User Read Only access to EEI created by others

11) Under **Additional User Rights:**

**Additional User Rights:**

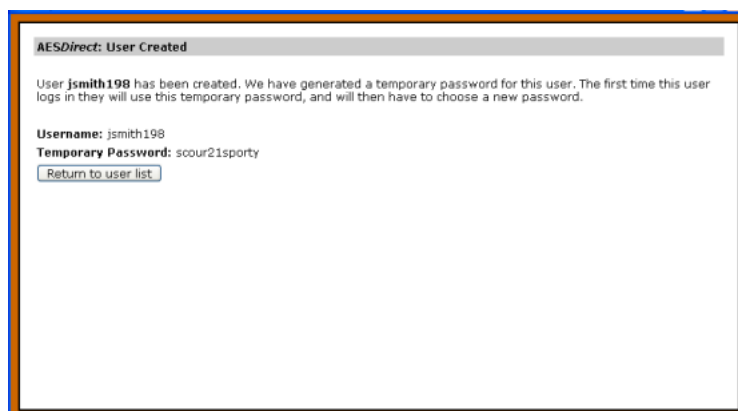
- ☐ This user can access the user management tools to create, modify, disable, and re-enable users (Mgr)

- a) Click the (Mgr) checkbox to give the User access to User Management tools. This will make the User a User Manager, with the ability to create, modify, disable, and re-enable Users

**Note:** Each AESDirect account is only allowed two (2) User Managers. If this checkbox is grayed out, you have already selected two User Managers. Questions about the number of User Managers you may create should be directed to AESDirect Technical Support.

Save User

12) Click 'Save User'



You will be brought to the **User Created** screen. The Username will be displayed and a temporary password assigned

13) Provide this information to the User by email or, preferably, telephone.

The screenshot shows the AESDirect login interface. At the top, there is a header with the AESDirect logo and the tagline "Reduce Exporting Stress with AES". Below the header, a warning banner reads: "\*\*WARNING\*\* \*\*WARNING\*\* \*\*WARNING\*\* \*\*WARNING\*\* \*\*WARNING\*\*". The main text area contains a disclaimer: "This is a Census Bureau computer system. Census Bureau computer systems are provided for the processing of official U.S. Government information only. All data contained within Census Bureau computer systems is owned by the Census Bureau, and may be monitored, intercepted, recorded, read, copied, or captured in any manner and disclosed in any manner, by authorized personnel. THERE IS NO RIGHT OF PRIVACY IN THIS SYSTEM. System personnel may disclose any potential evidence of crime found on Census Bureau computer systems to appropriate authorities. USE OF THIS SYSTEM BY ANY USER, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO THIS MONITORING, INTERCEPTION, RECORDING, READING, COPYING, CAPTURING, and DISCLOSURE OF COMPUTER ACTIVITY. Use of this computer without authorization or for unauthorized purposes is a violation of federal law and punishable by fines or imprisonment (Public Law 99-474)." Below this, another warning banner reads: "\*\*WARNING\*\* \*\*WARNING\*\* \*\*WARNING\*\* \*\*WARNING\*\* \*\*WARNING\*\*". The main message is "Your Password Has Expired". It states: "You need to change your password before you can log into AESDirect. Click 'Change Password' to change your password online, or 'Cancel' to return to the AESDirect homepage." At the bottom, there are two buttons: "Change Password" and "Cancel".

When the User first logs in to their account, they will be forced to change their password

The screenshot shows the "Change Password for User" form. The user name is "rpedersen". The form states: "Password cannot contain any dictionary words and it must meet the following criterias:". Below this, there are five criteria listed with red 'X' icons indicating they are not met:
 

- ✗ Password must be 12 characters long
- ✗ At least 1 character must be alphabetical AND at least 1 character must be a digit OR a non-alphanumeric character
- ✗ At least 6 characters must occur only once in a password
- ✗ Passwords cannot contain any string that is also contained in the username
- ✗ Passwords cannot contain any common strings such as a sequential series of letters (abcd) or a sequential series of numbers (1234) or pattern of numbers (2468)

 Below the criteria, there are three input fields: "Old Password:" (filled with dots), "New Password:", and "Confirm New Password:". At the bottom, there are two buttons: "Continue" and "Cancel".

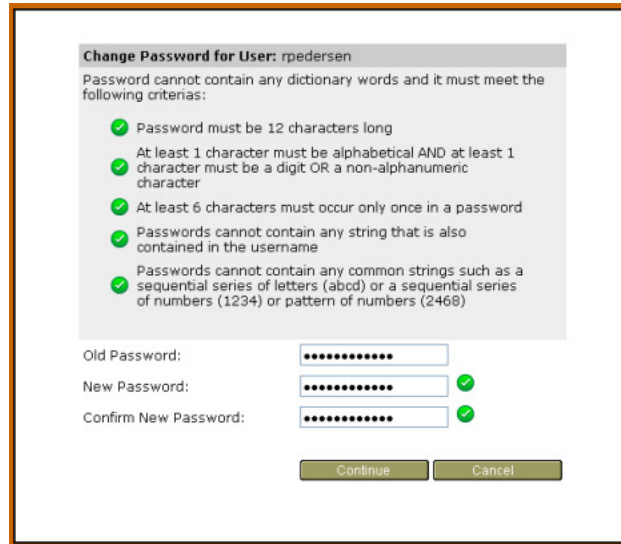
Users must enter the provided password in the 'Old Password' field.

All passwords must be at least 12 characters long and contain characters from 3 of these 4 groups:

- Lowercase Letters
- Uppercase Letters
- Numbers
- Special Characters: ! # \$ %

At least 6 of those characters may occur only once in the password

Please reference the **Password Rules** of this document for all password parameters.



**Change Password for User: rpedersen**

Password cannot contain any dictionary words and it must meet the following criterias:

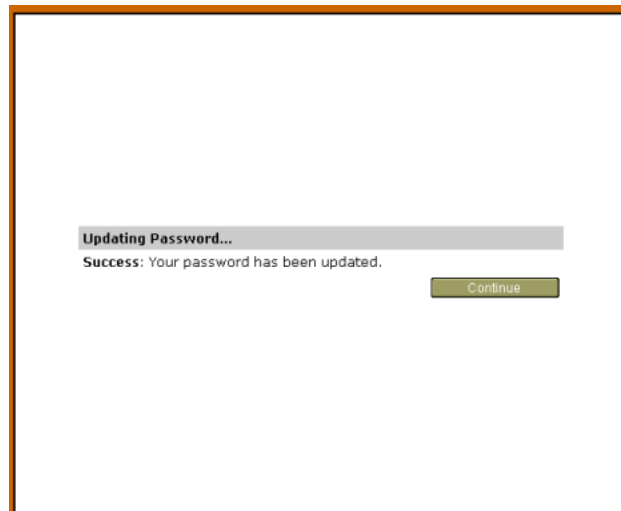
- ✓ Password must be 12 characters long
- ✓ At least 1 character must be alphabetical AND at least 1 character must be a digit OR a non-alphanumeric character
- ✓ At least 6 characters must occur only once in a password
- ✓ Passwords cannot contain any string that is also contained in the username
- ✓ Passwords cannot contain any common strings such as a sequential series of letters (abcd) or a sequential series of numbers (1234) or pattern of numbers (2468)

Old Password:

New Password:  ✓

Confirm New Password:  ✓

AESDirect will validate the password as the User creates it.



**Updating Password...**

**Success:** Your password has been updated.

Once the Users has successfully updated their password, that User will have access to the *AESDirect* functions you have granted to them.

## Create a User Manager

The role of a User Manager is very similar to that of the Account Administrator. A User Manager can serve as a point of contact for Users, and help:

- Establish new *AESDirect* Users
- Make changes to existing Users
- Reset passwords or reactivate disabled Users

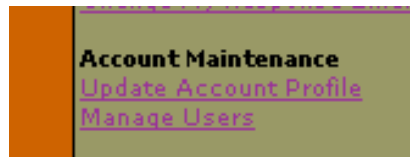
A User Manager is an *AESDirect* expert.

The only thing a User Manager may not do is act legally on behalf of the Account holder when contacting AESDirect. For instance, only an Account Administrator may contact AESDirect to reactivate a locked out Account.

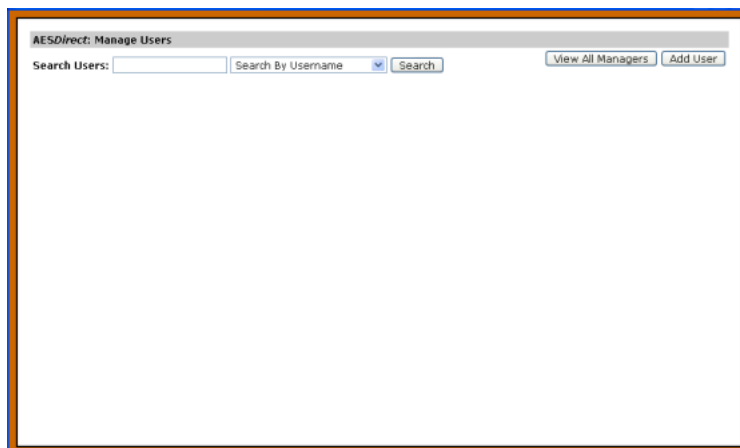
A User Manager can be a new or existing User. Your Company Account is limited, however, to only two (2) User Managers. Both the Account Administrator and a User Manager can create a User Manager.

To create a User Manager...

- 1) Login to *AESDirect*



- 2) Under **Account Maintenance**, Click 'Manage Users'



The **AESDirect: Manage Users** screen will open



- 3) Either follow the instructions to Create a New User and give that User Manager Permission or search for an existing User

**AESDirect: Manage Users**

Search Users:

- a) Enter at least one character of a search string

- Search By Username
- Search By E-Mail Address
- Search By First Name
- Search By Last Name

- b) Choose how you will 'Search by ...'

- Username
- E-Mail Address
- First Name
- Last Name

- c) Click 'Search'

A list of matches will be returned

**AESDirect: Manage Users**

Search Users:

Username	Quiz	App	Mgr	Admin	First Name	Last Name	E-Mail Address	Expiration
jsmith198	<a href="#">Edit</a>	<a href="#">Disable</a>	<a href="#">Reset Password</a>	Y	Jon	Smith	jsmith198@gmail.com	12/10/2008
jsmith99	<a href="#">Edit</a>	<a href="#">Disable</a>	<a href="#">Reset Password</a>	Y	John	Smith	jsmith@gmail.com	EXPIRED
jsmith999	<a href="#">Edit</a>	<a href="#">Disable</a>	<a href="#">Reset Password</a>	Y	John	Smith	jsmith99@yahoo.com	09/17/2008

- 4) Click 'Edit' next to the Username you would like to Modify

The **AESDirect: Edit User** screen will open

☐ This screen allows the user manager to edit user, add, delete, and enable users (Fig. 1)

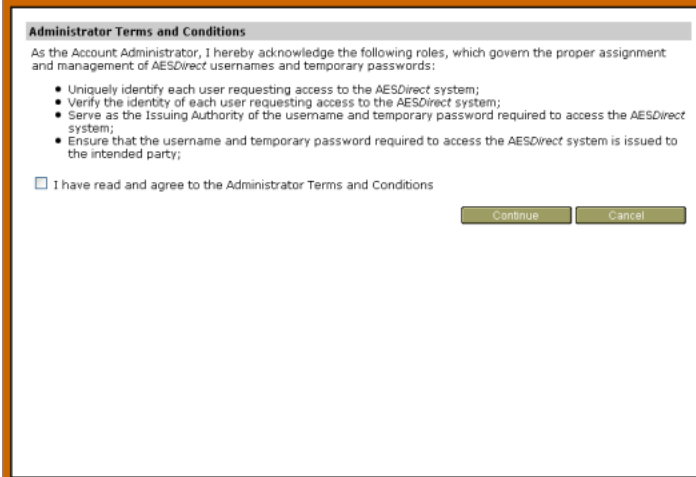
5) Click the (Mgr) checkbox

**Note:** Each AESDirect account is only allowed two (2) User Managers. If this checkbox is grayed out, you have already selected two User Managers. Questions about the number of User Managers you may create should be directed to AESDirect Technical Support.

6) Click 'Save User'

	Quiz App Mgr		
<a href="#">word</a>	Y	Y	Y
<a href="#">word</a>	Y	Y	
<a href="#">word</a>	Y		

The screen will refresh. Next to the Username a 'Y' should appear in the **Mgr** column. The User is now a User Manager.

A screenshot of a software dialog box titled "Administrator Terms and Conditions". The dialog box has a light gray header bar with the title. Below the header, the text reads: "As the Account Administrator, I hereby acknowledge the following roles, which govern the proper assignment and management of AESDirect usernames and temporary passwords:". This is followed by a bulleted list of four roles: "Uniquely identify each user requesting access to the AESDirect system;", "Verify the identity of each user requesting access to the AESDirect system;", "Serve as the Issuing Authority of the username and temporary password required to access the AESDirect system;", and "Ensure that the username and temporary password required to access the AESDirect system is issued to the intended party;". Below the list is a checkbox with the text "I have read and agree to the Administrator Terms and Conditions". At the bottom right of the dialog box are two buttons: "Continue" and "Cancel".

**Administrator Terms and Conditions**

As the Account Administrator, I hereby acknowledge the following roles, which govern the proper assignment and management of AESDirect usernames and temporary passwords:

- Uniquely identify each user requesting access to the AESDirect system;
- Verify the identity of each user requesting access to the AESDirect system;
- Serve as the Issuing Authority of the username and temporary password required to access the AESDirect system;
- Ensure that the username and temporary password required to access the AESDirect system is issued to the intended party;

☐ I have read and agree to the Administrator Terms and Conditions

Continue Cancel

When the new User Manager accesses the Account Maintenance functions the first time, they will be asked to confirm the **Terms and Conditions**.

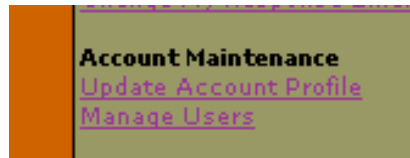
They must check the box to acknowledge that they have read and understand the Administrator Terms and Conditions, or they will not be able to access these functions.

## Reset Passwords

All Users forget their passwords. As an Account Administrator or a User Manager, it is your responsibility to reset these passwords. Resetting a Password is simple.

To reset a User's Password:

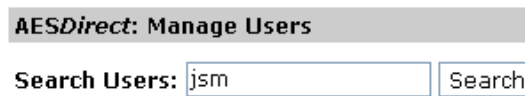
- 1) Login to *AESDirect*



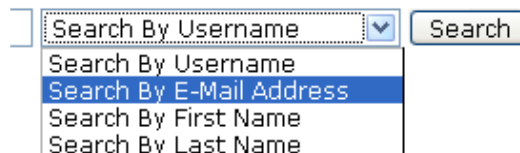
- 2) Under **Account Maintenance**, click 'Manage Users'

The **AESDirect: Manage Users** screen will open

- 3) Search for the User

A screenshot of a web form titled 'AESDirect: Manage Users' in a grey header bar. Below the header, the text 'Search Users:' is followed by a text input field containing the characters 'jsm'. To the right of the input field is a button labeled 'Search'.

- a) Enter at least the first character of a search string

A screenshot of a search dropdown menu. On the left is a small square checkbox. To its right is a dropdown menu with a blue border and a downward arrow on the right side. The menu is open, showing five options: 'Search By Username', 'Search By E-Mail Address' (which is highlighted with a blue background), 'Search By First Name', and 'Search By Last Name'. To the right of the dropdown menu is a button labeled 'Search'.

- b) Choose how you will 'Search by ...'

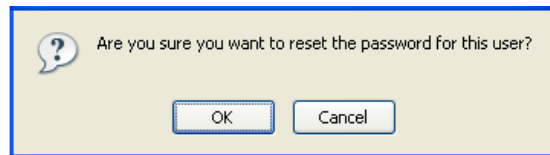
- Username
- E-Mail Address
- First Name
- Last Name

- c) Click 'Search'

Username			Qu
jsmith198	<a href="#">Edit</a>	<a href="#">Disable</a>	<a href="#">Reset Password</a>
jsmith99	<a href="#">Edit</a>	<a href="#">Disable</a>	<a href="#">Reset Password</a>
jsmith999	<a href="#">Edit</a>	<a href="#">Disable</a>	<a href="#">Reset Password</a>

A list of matches will be returned

4) Click 'Reset Password' next to the Username you would like to update



A box will open and ask you to confirm that you would like to reset the User's password

5) Click 'OK'



A new window will open. The password will be reset and a new temporary password displayed

6) Deliver this password directly to the User by email or, preferably, telephone.

The screenshot shows the AESDirect login interface. At the top, there are two circular logos: the U.S. Department of Commerce seal on the left and the AESDirect logo on the right. The title "AESDirect" is prominently displayed in a large, stylized font, with the tagline "Reduce Exporting Stress with AES" underneath it. Below the title, a series of asterisks and the word "WARNING" are repeated. A paragraph of text follows, stating that this is a Census Bureau computer system and that all data is owned by the Census Bureau. It also mentions that the system may be monitored and that there is no right of privacy. Below this text, another series of asterisks and the word "WARNING" are repeated. A section titled "Your Password Has Expired" is highlighted. It contains a message stating that the user needs to change their password before logging in. It provides two options: "Change Password" to change the password online, or "Cancel" to return to the homepage. At the bottom, there are two buttons: "Change Password" and "Cancel".

7) When the User attempts to login, they will be forced to change their password

The screenshot shows a "Change Password for User" dialog box. The title is "Change Password for User: rpedersen". Below the title, it states that the password cannot contain any dictionary words and must meet the following criteria:

- Password must be 12 characters long
- At least 1 character must be alphabetical AND at least 1 character must be a digit OR a non-alphanumeric character
- At least 6 characters must occur only once in a password
- Passwords cannot contain any string that is also contained in the username
- Passwords cannot contain any common strings such as a sequential series of letters (abcd) or a sequential series of numbers (1234) or pattern of numbers (2468)

Below the list of criteria, there are three input fields: "Old Password:", "New Password:", and "Confirm New Password:". The "Old Password" field is filled with dots. At the bottom, there are two buttons: "Continue" and "Cancel".

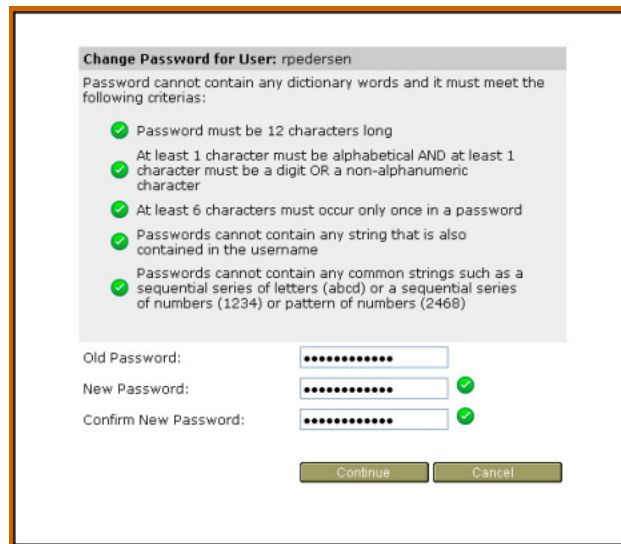
Users must enter the provided password in the 'Old Password' field.

All passwords must be at least 12 characters long and contain characters from 3 of these 4 groups:

- Lowercase Letters
- Uppercase Letters
- Numbers
- Special Characters: ! # \$ %

At least 6 of those characters may occur only once in the password

Please reference the **Password Rules** section of this document for all password parameters.



The screenshot shows a dialog box titled "Change Password for User: rpedersen". Below the title, a message states: "Password cannot contain any dictionary words and it must meet the following criterias:". A list of five criteria follows, each preceded by a green checkmark:

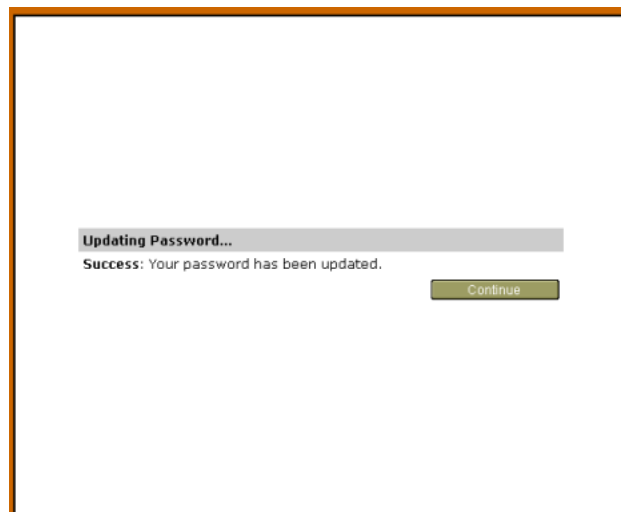
- ✓ Password must be 12 characters long
- ✓ At least 1 character must be alphabetical AND at least 1 character must be a digit OR a non-alphanumeric character
- ✓ At least 6 characters must occur only once in a password
- ✓ Passwords cannot contain any string that is also contained in the username
- ✓ Passwords cannot contain any common strings such as a sequential series of letters (abcd) or a sequential series of numbers (1234) or pattern of numbers (2468)

Below the list are three input fields:

- Old Password: [password field]
- New Password: [password field] ✓
- Confirm New Password: [password field] ✓

At the bottom are two buttons: "Continue" and "Cancel".

AESDirect will validate the password as the User creates it.



The screenshot shows a dialog box titled "Updating Password...". Below the title, a message states: "Success: Your password has been updated." At the bottom is a single button: "Continue".

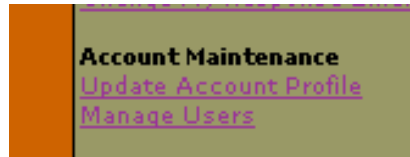
Once updated, the User will have access to your AESDirect Account.

## Disable a User

When a User is no longer responsible for filing EEI in *AESDirect* or leaves your company, you should disable the User. Disabled Users are not removed from *AESDirect* permanently, nor are their EEI. You may reactivate a disabled User at any time.

To disable a User Account

- 1) Login to *AESDirect*



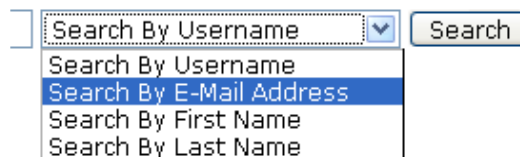
- 2) Under **Account Maintenance** click 'Manage Users'

The **AESDirect: Manage Users** screen will open

- 3) Search for the User

A screenshot of a web form titled 'AESDirect: Manage Users' in a grey header bar. Below the title, the text 'Search Users:' is followed by a text input field containing the characters 'jsm'. To the right of the input field is a button labeled 'Search'.

- a) Enter at least one character of a search string

A screenshot of a search dropdown menu. On the left is a small square icon. To its right is a dropdown menu with a dotted border. The menu is currently open, showing a list of search criteria: 'Search By Username' (selected), 'Search By E-Mail Address', 'Search By First Name', and 'Search By Last Name'. To the right of the dropdown menu is a button labeled 'Search'.

- b) Choose how you will 'Search by ...'

- Username
- E-Mail Address
- First Name
- Last Name

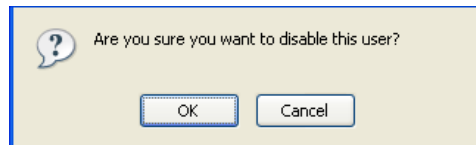
- c) Click 'Search'



Username			
jsmith198	<a href="#">Edit</a>	<a href="#">Disable</a>	<a href="#">Res</a>
jsmith99	<a href="#">Edit</a>	<a href="#">Disable</a>	<a href="#">Res</a>

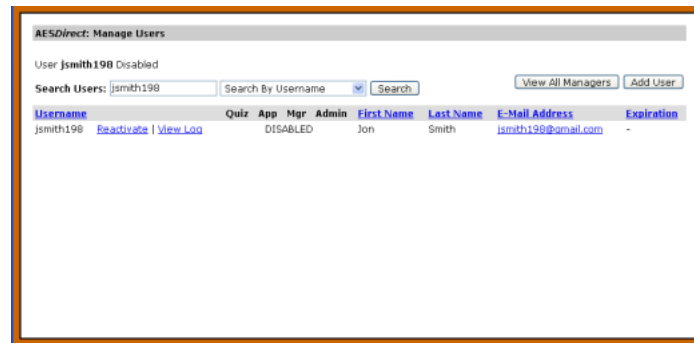
A list of matches will be returned.

- 4) Click 'Disable' next to the Username you would like disabled



A window will open and ask you to confirm

- 5) Click 'OK'



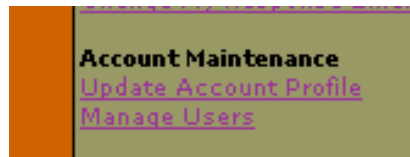
**DISABLED** will appear where a User's permissions are normally indicated.

## Reactivate a Disabled User

Users can be disabled for a number of reasons. If they have left the company, the Account Administrator or User Manager should disable them. Also, if a User has been in-active for more than 30 days, the User will be disabled. When a User is disabled, the User still exists in *AESDirect* and they can be reactivated at any time.

To reactivate a disabled User

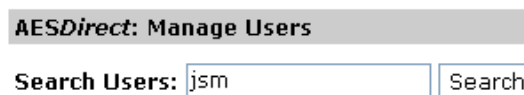
- 1) Login to *AESDirect*



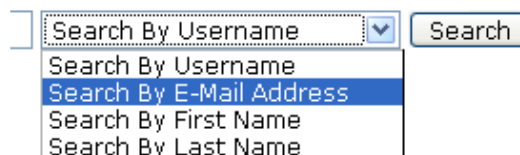
- 2) Under **Account Maintenance**, click 'Manage Users'

The **AESDirect: Manage Users** screen will open

- 3) Search for the User

A screenshot of a web form titled 'AESDirect: Manage Users' in a grey header bar. Below the title, the text 'Search Users:' is followed by a text input field containing the characters 'jsm'. To the right of the input field is a button labeled 'Search'.

- a) Enter at least one character of a search string

A screenshot of a search dropdown menu. The menu is open, showing a list of search criteria: 'Search By Username', 'Search By E-Mail Address' (which is highlighted with a blue background), 'Search By First Name', and 'Search By Last Name'. To the right of the dropdown is a button labeled 'Search'.

- b) Choose how you will 'Search by ...'

- Username
- E-Mail Address
- First Name
- Last Name

- c) Click 'Search'

Username	Quiz	App	Mgr	Admin	First Name	Last Name	E-Mail Address	Expiration
jsmith198	<a href="#">Reactivate</a>   <a href="#">View Log</a>			DISABLED	Jon	Smith	jsmith198@gmail.com	-
jsmith99	<a href="#">Edit</a>   <a href="#">Disable</a>   <a href="#">Reset Password</a>	Y			John	Smith	jsmith@gmail.com	EXPIRED
jsmith999	<a href="#">Edit</a>   <a href="#">Disable</a>   <a href="#">Reset Password</a>	Y	Y		John	Smith	jsmith99@yahoo.com	09/17/2008

A list of matches will be returned. **DISABLED** will appear where a Username's permissions are indicated.

If you do not know why the account is disabled click 'View Log'

Date/Time	IP Address	Action
09/11/2008 15:02:06.539946		Admin Action: User 'jsmith198' created BY rpedersen
09/11/2008 15:02:06.557868		Admin Action: User 'jsmith198' added to group 'Tutorial' BY rpedersen
09/11/2008 15:38:04.445981	192.168.32.53	Admin Action: Password Reset for User jsmith198 BY rpedersen
09/11/2008 17:14:33.081535	192.168.32.53	Admin Action: User jsmith198 Disabled BY rpedersen

**View Log** allows you to review the attempts the User or any other individual made to gain access to the account.

Below is the list of messages you may see when you access the **View Log** screen:

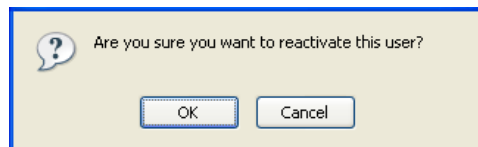
- Failed Login: Account Disabled
- Failed Login: Account Locked Out
- Failed Login: Password Mismatch
- Reset Password: Answer Security Question Failed (Password Recover System)
- System Message: User Account Now Locked Out
- Admin Action: Password Reset for User
- Admin Action: Locked Out User Unlocked
- Admin Action: Disabled User Reactivated
- Password Changed by User

Click 'Return to user list'

Search Users:

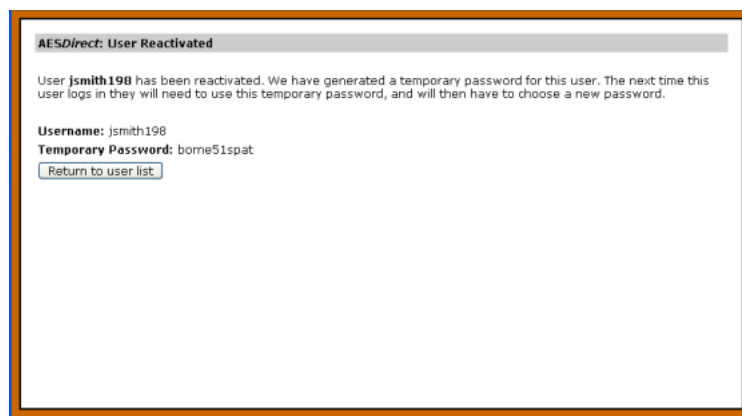
<a href="#">Username</a>	<a href="#">Q</a>
jsmith198	<a href="#">Reactivate</a>   <a href="#">View Log</a>

4) Click 'Reactivate'



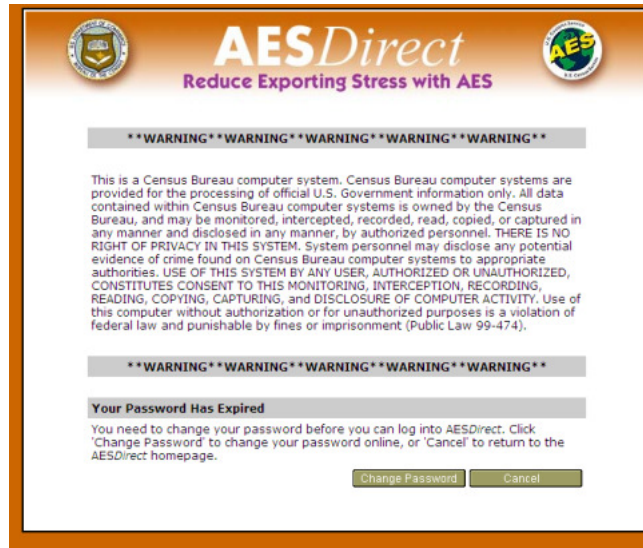
A window will open and ask you to confirm

5) Click 'OK'



A new window will open. The Username will be reactivated and a new temporary password will be displayed

6) Deliver this password directly to the User by email or, preferably, telephone.



7) When the User attempts to login, they will be forced to change their password

The screenshot shows the "Change Password for User: rpedersen" form. It lists several password requirements, each preceded by a red 'X' icon, indicating they are not met:
 

- Password must be 12 characters long
- At least 1 character must be alphabetical AND at least 1 character must be a digit OR a non-alphanumeric character
- At least 6 characters must occur only once in a password
- Passwords cannot contain any string that is also contained in the username
- Passwords cannot contain any common strings such as a sequential series of letters (abcd) or a sequential series of numbers (1234) or pattern of numbers (2468)

 Below the requirements, there are three input fields: "Old Password:" (filled with dots), "New Password:", and "Confirm New Password:". At the bottom, there are two buttons: "Continue" and "Cancel".

Users must enter the provided password in the 'Old Password' field.

All passwords must be at least 12 characters long and contain characters from 3 of these 4 groups:

- Lowercase Letters
- Uppercase Letters
- Numbers
- Special Characters: ! # \$ %

At least 6 of those characters may occur only once in the password

Please reference the **Password Rules** of this document for all password parameters.

**Change Password for User: rpedersen**

Password cannot contain any dictionary words and it must meet the following criteria:

- ✓ Password must be 12 characters long
- ✓ At least 1 character must be alphabetical AND at least 1 character must be a digit OR a non-alphanumeric character
- ✓ At least 6 characters must occur only once in a password
- ✓ Passwords cannot contain any string that is also contained in the username
- ✓ Passwords cannot contain any common strings such as a sequential series of letters (abcd) or a sequential series of numbers (1234) or pattern of numbers (2468)

Old Password:  .....

New Password:  ..... ✓

Confirm New Password:  ..... ✓

AESDirect will validate the password as the User creates it.

**Updating Password...**

**Success:** Your password has been updated.

## Reactivate a Locked Out User

Users who attempt to log in to *AESDirect* with their Username but make 5 consecutive invalid attempts within 15 minutes will, as a security precaution, be locked out.

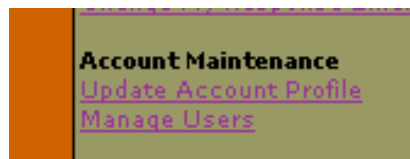


The screenshot shows the AESDirect login interface. At the top right is a link for [Need Help?](#). Below it are two input fields: 'Username:' containing 'rpedersen' and 'Password:' containing ten dots. A red error message states: 'No user account found for the username and password entered'. Below this, it says 'You can try 3 more time(s) before your user account is locked out'. Further down, it advises: 'Please check that you have entered the correct username and remember that passwords are case sensitive.' and 'Contact your account administrator or a user manager if you need assistance.' A 'Continue' button is located below the text. At the bottom, a note reads: 'Please remember that passwords are case sensitive. For users that have upgraded to the new account administration tools, 5 consecutive invalid login attempts will result in your username being locked out.'

It is the responsibility of the Account Administrator or the User Manager to reactivate Locked Out Users. Users can only be unlocked following a 15 minute 'time out.'

To reactivate a locked out User...

- 1) Login to *AESDirect*



- 2) Under **Account Maintenance**, click 'Manage Users'

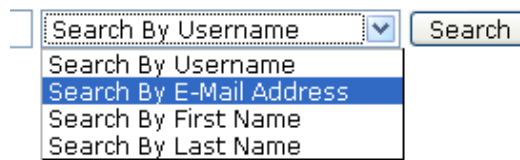
The **AESDirect: Manage Users** screen will open

- 3) Search for the User



The screenshot shows the 'AESDirect: Manage Users' header. Below it is a search bar with the text 'Search Users:' followed by an input field containing 'jsm' and a 'Search' button.

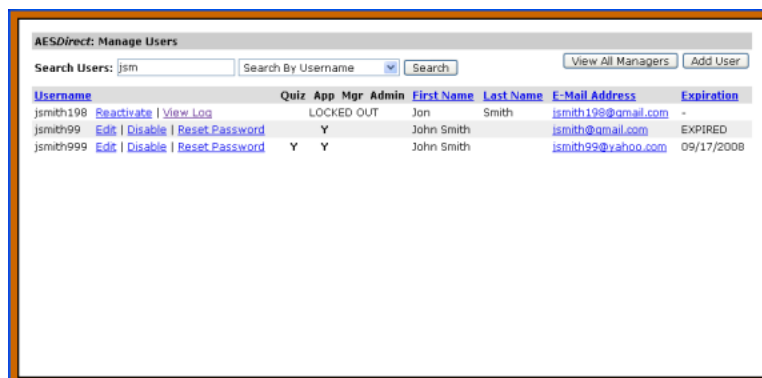
- a) Enter at least one character of a search string



b) Choose how you will 'Search by ...'

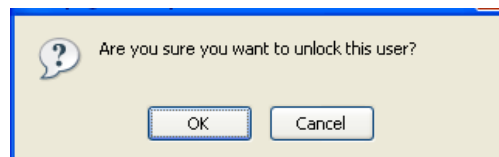
- Username
- E-Mail Address
- First Name
- Last Name

c) Click 'Search'



A list of matches will be returned. **Locked Out** will appear where a Username's permissions are indicated.

4) Click 'Reactivate'

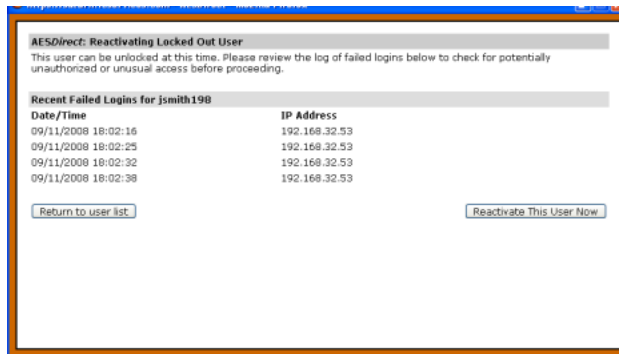


A window will open and ask you to confirm

5) Click 'OK'

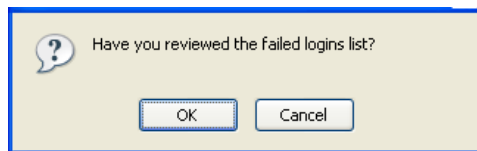
The **AESDirect: Reactivating Locked Out User** screen will open and display all recent attempts to login. You will only be able to reactivate this User if it has been 15 minutes since the last failed attempt.





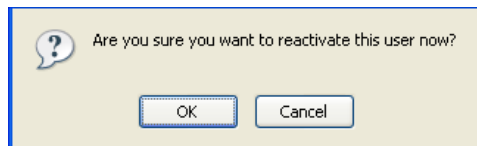
**Recent Failed Logins** lets you to review the number of attempts the User or any other individual made to try to gain access to the account. If the number of attempts is significantly more than the five that would result in a lockout, your AESDirect Account may be subject to a malicious attack. If you suspect you are the victim of an attack, contact AESDirect Technical Support immediately.

- 6) Review the log in attempts again to identify any abnormalities
- 7) If all seems right, click 'Reactivate This User Now'



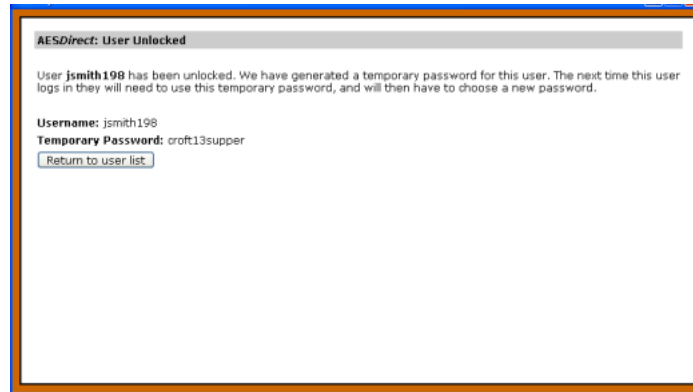
A window will open and ask you to confirm you have reviewed the failed Logins list

- 8) Click 'OK'



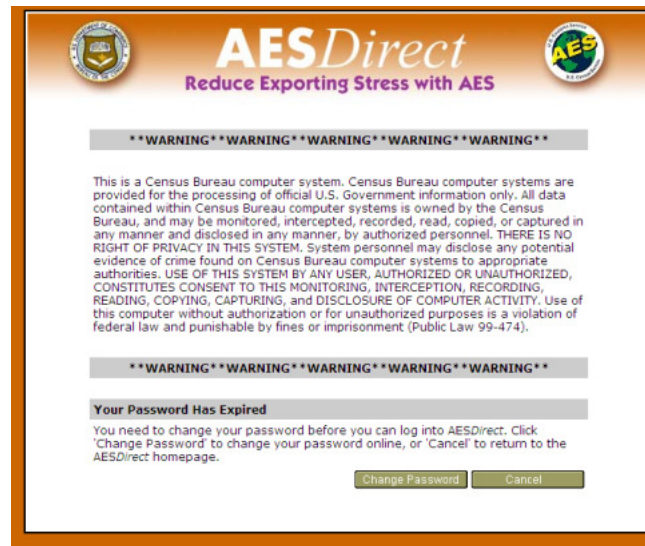
Another window will open and ask if you are sure you would like to reactivate the User.

- 9) Click 'OK'



A new window will open. The password will be reset and a new temporary password displayed

10) Deliver this password directly to the User.



When the User next logs in to their account, they will be forced to change their password

**Change Password for User: rpedersen**

Password cannot contain any dictionary words and it must meet the following criterias:

- ✗ Password must be 12 characters long
- ✗ At least 1 character must be alphabetical AND at least 1 character must be a digit OR a non-alphanumeric character
- ✗ At least 6 characters must occur only once in a password
- ✗ Passwords cannot contain any string that is also contained in the username
- ✗ Passwords cannot contain any common strings such as a sequential series of letters (abcd) or a sequential series of numbers (1234) or pattern of numbers (2468)

Old Password:

New Password:

Confirm New Password:

Users must enter the provided password in the ‘Old Password’ field.

All passwords must be at least 12 characters long and contain characters from 3 of these 4 groups:

- Lowercase Letters
- Uppercase Letters
- Numbers
- Special Characters: ! # \$ %

At least 6 of those characters may occur only once in the password

Please reference the **Password Rules** section of this document for all password parameters.

**Change Password for User: rpedersen**

Password cannot contain any dictionary words and it must meet the following criterias:

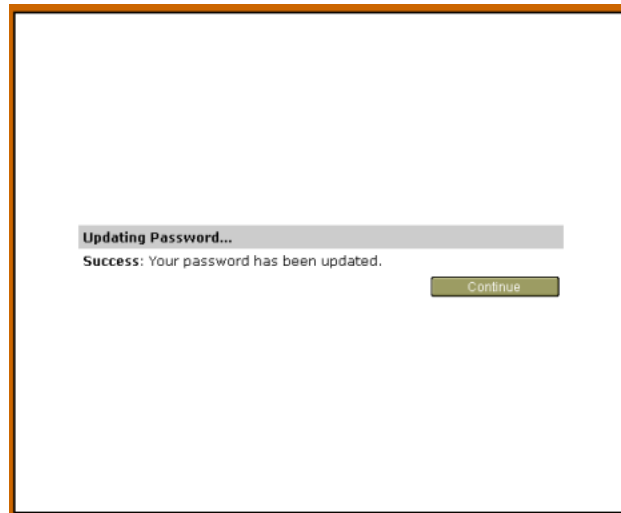
- ✓ Password must be 12 characters long
- ✓ At least 1 character must be alphabetical AND at least 1 character must be a digit OR a non-alphanumeric character
- ✓ At least 6 characters must occur only once in a password
- ✓ Passwords cannot contain any string that is also contained in the username
- ✓ Passwords cannot contain any common strings such as a sequential series of letters (abcd) or a sequential series of numbers (1234) or pattern of numbers (2468)

Old Password:

New Password:  ✓

Confirm New Password:  ✓

AESDirect will validate the password as the User creates it.



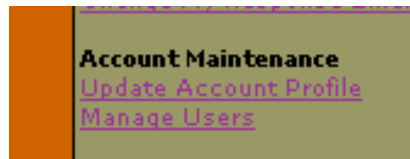
Once updated, the User will have access to your AESDirect Account.

## Change an Account Administrator

As with all Users, when the Account Administrator leaves, their account will need to be disabled. Unlike Users or User Managers, your company must take additional measures identify a new Account Administrator in *AESDirect*, as they are the individual directly responsible for *AESDirect* maintenance.

To Change an Account Administrator...

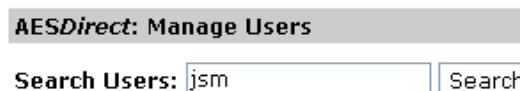
- 1) Login to *AESDirect*



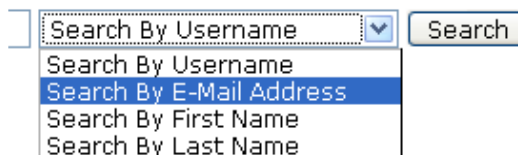
- 2) Under **Account Maintenance**, click 'Manage Users'

The **AESDirect: Manage Users** screen will open

- 3) Search for the User



- a) Enter at least one character of a search string



- b) Choose how you will 'Search by ...'

- Username
- E-Mail Address
- First Name
- Last Name

- c) Click 'Search'

**AESDirect: Manage Users**

Search Users:  Search By Username

Username	Quiz	App	Mgr	Admin	First Name	Last Name	E-Mail Address	Expiration	
rpedersen	<a href="#">Edit</a>	<a href="#">Disable</a>	<a href="#">Reset Password</a>	Y	Y	Y	Robert Pedersen	<a href="mailto:rpedersen@tradeqate2000.com">rpedersen@tradeqate2000.com</a>	09/22/2010
rpedersen1	<a href="#">Edit</a>	<a href="#">Disable</a>	<a href="#">Reset Password</a>	Y	Y		Rob Test	<a href="mailto:rob@donsoilitude.net">rob@donsoilitude.net</a>	EXPIRED

A list of matches will be returned.

4) Click 'Edit' next to the User you would like to make the Account Administrator

**AESDirect: Edit User**

Utilities: [View Log](#) ; [Transfer Account Administrator Role to This User](#)

Username: rpedersen

First Name:

Last Name:

E-Mail Address:

Allow this user to access:

- ☒ This user can access the certification quizzes. Once they pass the certification quiz they will be give access to the AESDirect application (Quiz)
- ☒ This user can access AESDirect application (App)
- ☐ This user can access the user management tools to create, modify, disable, and re-enable users (Mgr)

Within the AESDirect application this user may:

- ☒ This user can File EEI (This includes editing, resubmitting, and canceling EEI)
- ☐ This user can only View EEI

5) Click 'Transfer Account Administrator Role to This User'

**AESDirect: Transfer Account Admin**

Please enter the contact details for the new Account Administrator. When you complete this form you will no longer have administrator rights to your AESDirect account and any changes will have to be made by the user you have nominated below.

Username: rpedersen

First Name:

Last Name:

E-Mail Address:

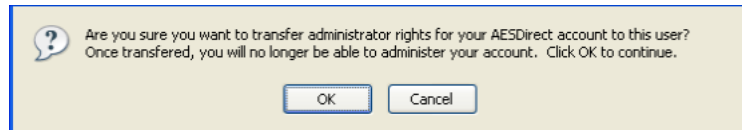
Phone Number:

Fax Number:

The **AESDirect: Transfer Account Admin** window will open.

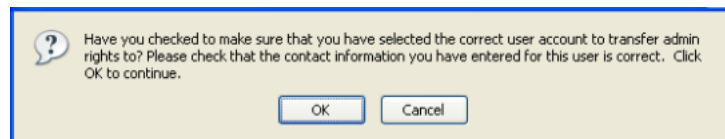
6) Complete any profile information that may be missing. All fields must be completed.

7) Click 'Transfer Account Administration'



You will be asked to confirm the change of Account Administrator a first time

8) Click 'OK'



You will be asked to confirm the change of Account Administrator a second time

9) Click 'OK'



You will see **Admin Transfer Successful** if there are no problems. Account Administrator privileges will transfer to the selected User. You will no longer be an Account Administrator.

10) Check on the Status of your changes.

**Account Maintenance**  
Update Account Profile  
Manage Users

11) Under **Account Maintenance**, click 'Update Account Profile'

**Administrator**

<b>Name</b>	Robert Pedersen
<b>Email</b>	<b><a href="mailto:rpedersen@tradegate2000.com">rpedersen@tradegate2000.com</a></b>
<b>Phone</b>	(301) 562-7790
<b>Fax</b>	(301) 562-7791

The new Account Administrator contact information should be listed.



## WHAT HAPPENS IF THE ACCOUNT ADMINISTRATOR LEAVES?

If the User designated as an Account Administrator leaves the company and does not nominate a replacement Account Administrator before their password expires, there are manual steps you can take to have a new Account Administrator nominated.

FAX the Technical Request Form to **Fax # (301) 562-7795**

The form is available here:

<http://aesdirect.census.gov/support/AESDirectTechnicalAssistanceFaxForm.pdf>

This request must come from an authorized company officer (President, CEO, etc.) and signed by that company officer. The letter must specifically request that you wish to nominate a new Account Administrator as the one on file is no longer employed by the company.

Include the following:

- Company Name
  - Company ID Number (EIN, SSN, or DUNS)
  - *AESDirect* Username. Either
    - New Username you wish to be created; or
    - Existing Username
  - The new administrator information:
    - Name
    - Phone Number
    - Fax Number
    - E-Mail Address
    - Mailing Address
  - Signature & Title of the person requesting the change
- 1) Once we have received your fax, we will contact the new Account Administrator and provide a Username, if new, and a Password.
  - 2) The New Account Administrator must login. They will be forced to reset their password

All passwords at least 12 characters long and contain characters from 3 of these 4 groups

- Lowercase Letters
- Uppercase Letters
- Numbers
- Special Characters: ! # \$ %

Please reference the **Password Rules** section of this document for all password parameters.

- 4) Under Account Maintenance, click 'Update Account Profile' to verify your information is correct.